R. W. Spekkens[1] and T. Rudolph[2]
[1] *Department of Physics, University of Toronto, 60 St. George Street, Toronto, Ontario, Canada, M5S 1A7*
[2] *Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Vienna, Austria*
(June 6, 2001)

Although it is impossible for a bit commitment protocol to be both arbitrarily concealing and arbitrarily binding, it *is* possible for it to be both *partially* concealing and *partially* binding. This means that Bob cannot, prior to the beginning of the unveiling phase, find out everything about the bit committed, and Alice cannot, through actions taken after the end of the commitment phase, unveil whatever bit she desires. We determine upper bounds on the degrees of concealment and bindingness that can be achieved simulatneously in *any* bit commitment protocol, although it is unknown whether these can be saturated. We *do*, however, determine the maxima of these quantities in a restricted class of bit commitment protocols, namely those wherein all the systems that play a role in the commitment phase are supplied by Alice. We show that these maxima can be achieved using a protocol that requires Alice to prepare a pair of systems in an entangled state, submit one of the pair to Bob at the commitment phase, and the other at the unveiling phase. Finally, we determine the form of the trade-off that exists between the degree of concealment and the degree of bindingness given various assumptions about the purity and dimensionality of the states used in the protocol.

I. INTRODUCTION

Bit commitment(BC) is a cryptographic primitive involving two mistrustful parties, Alice and Bob, wherein one seeks to have Alice submit an encoded bit of information to Bob in such a way that Bob cannot reliably identify the bit before Alice decodes it for him, and Alice cannot reliably change the bit after she has submitted it. In other words, Bob is interested in binding Alice to some commitment, and Alice is interested in concealing this commitment from Bob. Mayers [1], and independently Lo and Chau [2], have shown that a BC protocol that is both concealing and binding is impossible [3]. Nonetheless, it *is* possible to devise a BC protocol that is both *partially* concealing and *partially* binding, that is, one wherein if Alice is honest then the probability that Bob can estimate her commitment correctly is strictly less than 1, and if Bob is honest then the probability that Alice can unveil whatever bit she desires is strictly less than 1. This paper addresses the problem of determining the *optimal* degrees of concealment and bindingness that can be achieved simultaneously in quantum bit commitment protocols.

Building upon the work of Mayers and Lo and Chau, we establish an upper bound on the degrees of concealment and bindingness of all BC protocols. It is unclear at this time whether or not this upper bound can be saturated. Nonetheless, we *are* able to provide a saturable upper bound for a more restricted class of BC protocols, namely protocols wherein Alice initially holds all of the systems that play a role in the commitment phase of the protocol. We also introduce a new kind of BC protocol that achieves this maximum. The protocol essentially consists of Alice preparing two systems in an entangled state, submitting one half to Bob at the commitment phase, and submitting the other half at the unveiling phase. We show that in such protocols the maximum achievable degree of bindingness is related in a simple way to the fidelity between the reduced density operators for the systems held by Bob at the end of the commitment phase.

BC appears as a primitive in the protocols of many different cryptographic tasks between mistrustful parties. As such, the kinds of security that can be achieved in BC has implications for the kinds of security that can be achieved in these other tasks. In this paper we consider only the implications of our results to the task of coin tossing. [5] [6].

II. DEGREES OF CONCEALMENT AND BINDINGNESS

A bit commitment protocol involves three phases, which are called the commitment phase, the holding phase and the unveiling phase. During the commitment phase, Alice and Bob engage in some number of rounds of communication, with at least one communication from Alice to Bob. The period after the end of the commitment phase and prior to the beginning of the unveiling phase is called the holding phase, and may be of arbitrary duration. During the unveiling phase, there is again some number of rounds of communication, with at least one communication from Alice to Bob. At the end of the unveiling phase, an honest Bob performs a measurement that has three outcomes, labelled '0','1' and 'fail', corresponding respectively to Alice unveiling a 0, Alice unveiling a 1 and Alice being caught cheating. The protocol

specifies the sequence of actions an honest Alice performs in order to commit to a bit b, and guarantees that if she follows the actions for committing a bit b then Bob's measurement at the end of the unveiling phase yields the outcome b with certainty.

To discuss the security of BC protocols, it is useful to introduce two quantities which we shall call Alice's *control* and Bob's *information gain*. These quantities are defined under the assumption that the other party is honest, and depend on the sequence of actions performed by the party in question. Alice's control is meant to quantify the extent to which she can influence the outcome of Bob's measurement beyond what she could accomplish by following the honest protocol. Bob's information gain is meant to quantify his ability to estimate Alice's commitment (prior to the unveiling phase) beyond what he could accomplish by following the honest protocol.

We now present the specific measures of control and information gain which we make use of in this paper. We take our measure of Alice's control for the sequence of actions S^A, which we denote by $C\left(S^A\right)$, to be the difference between her probability of unveiling the bit of her choosing when she performs S^A and this probability when she is honest,

$$C(S^A) = P_{\mathrm{U}}(S^A) - P_{\mathrm{U}}\left(S^A_{\mathrm{honest}}\right).$$

We take our measure of Bob's information gain for the sequence of actions S^B, which we denote by $G\left(S^B\right)$, to be the difference between his probability of estimating Alice's commitment correctly when he performs S^B and this probability when he is honest,

$$G\left(S^B\right) = P_{\mathrm{E}}(S^B) - P_{\mathrm{E}}\left(S^B_{\mathrm{honest}}\right).$$

In this paper we assume for simplicity that Alice will desire to unveil bit 0 and bit 1 with equal probabilities, so that $P_{\mathrm{U}}\left(S^A_{\mathrm{honest}}\right) = 1/2$, and that Bob has no prior information on which bit she has committed, so that $P_{\mathrm{E}}\left(S^B_{\mathrm{honest}}\right) = 1/2$. Thus, $C(S^A)$ and $G(S^B)$ vary between 0 and $1/2$.

We quantify the degrees of concealment and bindingness in a BC protocol by Bob's maximum information gain and Alice's maximum control, defined respectively by

$$G^{\max} \equiv \max_{S^B} G\left(S^B\right),$$
$$C^{\max} \equiv \max_{S^A} C\left(S^A\right).$$

A protocol is said to be *partially concealing* if Bob's maximum information gain is strictly less than complete information gain, $G^{\max} < 1/2$; it is said to be *perfectly concealing* if his information gain is zero, $G^{\max} = 0$; finally, it is said to be *arbitrarily concealing* or simply *concealing* if his information gain can be made arbitrarily small by increasing the value of a security parameter, $G^{\max} \leq \varepsilon$, where $\varepsilon \to 0$ as $N \to \infty$ [7]. We introduce similar definitions for degrees of security against Alice. A protocol is said to be *partially binding* if Alice's maximal control is strictly less than complete control, $C^{\max} < 1/2$; it is said to be *perfectly binding* if her control is zero, $C^{\max} = 0$; finally, it is said to be *arbitrarily binding* or simply *binding* if her control can be made arbitrarily small by increasing the value of a security parameter, $C^{\max} \leq \delta$, where $\delta \to 0$ as $N \to \infty$.

If a degree of security (such as concealment or bindingness) can be guaranteed by assuming only the laws of physics (and the integrity of a party's laboratory), then it is said to hold *unconditionally*. In this paper, we shall only be concerned with unconditional security. Thus, every time we assign some degree of security (such as concealment or bindingness) to a protocol, it is implied that the protocol has this feature unconditionally.

To understand the degree to which a protocol can be made concealing or binding we must answer the following questions:

- What is Bob's maximal information gain, and what strategy achieves this maximum? That is, find $G^{\max}$, and find $S_B^{\max}$ such that $G(S_B^{\max}) = G^{\max}$.
- What is Alice's maximal control, and what strategy achieves this maximum? That is, find $C^{\max}$, and find $S_A^{\max}$ such that $C(S_A^{\max}) = C^{\max}$.

In another paper [8], we provide answers to these questions for BC protocols that are generalizations of the BB84 BC protocol [9]. In this paper, we provide the complete solution for a different type of BC protocol, which we call a *purification* BC protocol.

The above questions involve an optimization over strategies. We will also be interested in optimizing over protocols. Specifically, we wish to answer the following question:

- For a given class of protocols, what is the *minimum* Alice's maximal control can be made for a given value of Bob's maximal information gain, and which protocol in the class achieves this minimum? In other words, denoting protocols by $\mathcal{P}$ and the given class of protocols by $\mathcal{K}$, find $\min_{\mathcal{P}\in\mathcal{K}} C^{\max}(G^{\max}, \mathcal{P})$ and find $\mathcal{P}^{\mathrm{opt}}$ such that $C^{\max}(G^{\max}, \mathcal{P}^{\mathrm{opt}}) = \min_{\mathcal{P}\in\mathcal{K}} C^{\max}(G^{\max}, \mathcal{P})$.

If this question can be answered for every value of $G^{\max}$, then one obtains the optimal trade-off relation between $C^{\max}$ and $G^{\max}$ among protocols $\mathcal{P}$ in class $\mathcal{K}$. The optimal trade-off for a given class of protocols is a convenient way of expressing the maximum degrees of concealment and bindingness that can be achieved with such protocols.

In this paper, we determine a lower bound on the optimal trade-off relation between $C^{\max}$ and $G^{\max}$ for the class of *all* BC protocols. Unfortunately, we have not determined whether this lower bound is saturable or not. However, we *do* find the optimal trade-off relation for

a restricted class of BC protocols, which we call *Alice-supplied* BC protocols. The generalized BB84 BC protocols and the purification BC protocols mentioned above both fall into this class. In fact, we show that the purification BC protocols are optimal within this class. These protocols will be defined precisely in the next section.

III. BC PROTOCOLS

In order to perform optimizations over all quantum BC protocols, it is necessary to have a completely general model of such protocols. We make use of the following model for cryptographic protocols implemented between two mistrustful parties [1]. The Hilbert space required to describe the protocol is the tensor product of the Hilbert spaces for all the systems that play a role in the protocol. Every action taken by a party in their laboratory corresponds to that party performing a unitary operation on the systems in their possession. Every communication corresponds to a party sending some subset of the systems in their possession to the other party (it follows that the mere transmission of information from one party to the other does not change the quantum state of the total system, but does change the Hilbert space upon which the parties can implement their unitary operations). It is assumed that the total system is initially in a pure state.

It has been previously argued [1] that this model is completely general. It incorporates the possibility of random choices and measurements during the protocol, since these can always be kept at the quantum level until the end without any loss of generality. A random choice is performed at the quantum level by implementing a unitary transformation that is conditioned upon the state of an ancilla prepared initially in a particular superposition of states. Measurements are performed at the quantum level by unitarily coupling the system to be measured to an ancilla that is prepared in some fixed initial pure state.

In the case of BC, the most general protocol may involve many rounds of communication during the commitment phase. Denoting the number of rounds by n, denoting Alice's honest sequence of operations for committing a bit b by $\{W_{b,1}, ..., W_{b,n}\}$, and denoting Bob's honest sequence of operations by $\{W'_1, ..., W'_n\}$, the total unitary operation they jointly implement is

$$W_b \equiv W'_n W_{b,n} \cdots W'_2 W_{b,2} W'_1 W_{b,1}.$$

The transmissions that occur in each round will determine the Hilbert space over which $W_{b,i}$ and W'_i act nontrivially. Thus, despite the fact that we have assumed that Alice implements the first unitary operation, this operation could be trivial and it remains arbitrary which party is first to submit a sytem to the other party. If the initial state of all systems is denoted by $|\psi_{\text{init}}\rangle$, then the state at the holding phase if both parties are honest is

$$|\psi_b\rangle \equiv W_b |\psi_{\text{init}}\rangle .$$

The reduced density operator for Bob's system at the holding phase is therefore

$$\rho_b = Tr \left(|\psi_b\rangle \langle\psi_b| \right),$$

where the trace is over all the systems that end up in Alice's possession at the holding phase.

During the unveiling phase, a similar process occurs. Denoting the number of rounds by m, denoting Alice's honest sequence of operations given that she committed to bit b by $\{V_{b,1}, ..., V_{b,n}\}$, and denoting Bob's honest sequence of operations by $\{V'_1, ..., V'_n\}$, the total unitary operation they jointly implement is

$$V_b \equiv V'_n V_{b,n} \cdots V'_2 V_{b,2} V'_1 V_{b,1}.$$

Thus, if both parties are honest, the state of the total system at the end of the unveiling phase is

$$|\psi_b^{\text{unv}}\rangle \equiv V_b |\psi_b\rangle . \tag{1}$$

The protocol ends with Bob performing a three-outcome projective measurement $\{\Pi_0, \Pi_1, \Pi_{\text{fail}}\}$ on the systems in his possession. If both parties are honest, then whenever Alice commits to a bit b, the measurement must have outcome b with probability 1. This implies that $|\psi_0^{\text{unv}}\rangle$ and $|\psi_1^{\text{unv}}\rangle$ must be orthogonal,

$$\langle\psi_0^{\text{unv}}|\psi_1^{\text{unv}}\rangle = 0,$$

and that $|\psi_b^{\text{unv}}\rangle$ must be an eigenstate of Π_b with eigenvalue 1,

$$\Pi_b |\psi_b^{\text{unv}}\rangle = |\psi_b^{\text{unv}}\rangle . \tag{2}$$

As mentioned earlier, we will be interested in a restricted class of BC protocols, which we call *Alice-supplied* BC protocols. These protocols impose no restrictions on the details of the unveiling phase and may involve an arbitrary number of rounds of communication between Alice and Bob during the commitment phase. However, it is required that *all* of the systems that Bob makes use of during the commitment phase are supplied by Alice. The class of Alice-supplied BC protocols includes the generalized BB84 BC protocols, defined in Ref. [8], as well as the purification BC protocols defined below. An example of a protocol that falls *outside* this class is one wherein at the beginning of the commitment phase Bob submits to Alice a system that is entangled with one he keeps in his possession, and Alice encodes her commitment in the unitary transformation she performs upon this system before resubmitting it to Bob.

We now provide a precise definition of a purification BC protocol.

A purification BC protocol. Such a protocol makes use of just two systems, which we shall call the token system and the proof system (since one is the token of Alice's

commitment and the other is the proof of her commitment). These are associated with Hilbert spaces $\mathcal{H}_p$ and $\mathcal{H}_t$. A purification BC protocol also specifies two orthogonal states $|\chi_0\rangle$ and $|\chi_1\rangle$ defined on $\mathcal{H}_p \otimes \mathcal{H}_t$. The honest actions are as follows.

1. At the commitment phase, Alice prepares the two systems in the state $|\chi_b\rangle$ in order to commit to bit b, and sends the token system to Bob.

2. At the unveiling phase, Alice sends the proof system to Bob, and Bob performs a measurement of the projector-valued measure $\{\Pi_0, \Pi_1, \Pi_{\text{fail}}\}$, where $\Pi_b = |\chi_b\rangle \langle\chi_b|$.

So we see there is only a single communication from Alice to Bob during both the commitment and the unveiling phases. In the notation of the general model presented above, W_b transforms $|\psi_{\text{init}}\rangle$ to $|\psi_b\rangle = |\chi_b\rangle$, and $V_b = I$ so that $|\psi_b^{\text{unv}}\rangle = |\psi_b\rangle = |\chi_b\rangle$.

We call this a purification BC protocol, since at the unveiling phase an honest Alice is required to provide Bob with a purification of the state that he received from her during the commitment phase.

IV. MEASURES OF DISTINGUISHABILITY FOR DENSITY OPERATORS

Two measures of the distinguishability of density operators will be important in the present work: the trace distance and the fidelity, defined respectively by [10]

$$D(\rho, \sigma) = \frac{1}{2} Tr |\rho - \sigma|,$$

and

$$F(\rho, \sigma) = Tr \left|\sqrt{\rho}\sqrt{\sigma}\right|,$$

where $|A| = \sqrt{A^\dagger A}$.

We will find the following relations between these two measures to be very useful [10]. For any two density operators, the fidelity and the trace distance satisfy

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma), \tag{3}$$

and

$$D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2} \tag{4}$$

The second inequality is saturated for any pair of pure states, that is,

$$D(|\psi\rangle, |\chi\rangle) = \sqrt{1 - F(|\psi\rangle, |\chi\rangle)^2}, \tag{5}$$

for all $|\psi\rangle$ and $|\chi\rangle$. A stronger lower bound for the trace distance between ρ and σ exists if one of the density operators is pure. Specifically,

$$1 - F^2(\rho, |\psi\rangle) \leq D(\rho, |\psi\rangle). \tag{6}$$

This stronger lower bound also applies to the mixed states of qubits. More precisely, we have the following result.

Lemma 1 For pairs of density operators ρ, σ whose supports lie in a single 2-dimensional Hilbert space,

$$1 - F^2(\rho, \sigma) \leq D(\rho, \sigma).$$

The proof of this is presented in the Appendix. All of the above inequalities can be saturated. Explicit examples will be presented in section VI.

Finally, we present some properties of the fidelity that will be useful for the present investigation. Uhlmann's theorem [11] states that the fidelity between two density operators is equal to the overlap of two maximally parallel purifications of these density operators. Thus, if ρ and σ are density operators on a Hilbert space $\mathcal{H}$, $|\psi\rangle$ and $|\chi\rangle$ are arbitrary purifications of ρ and σ on $\mathcal{H}' \otimes \mathcal{H}$, and U is a unitary transformation on $\mathcal{H}$, then

$$F(\rho, \sigma) = \max_U |\langle\psi| U \otimes I |\chi\rangle|. \tag{7}$$

Another critical property is given by the following lemma.

Lemma 2 The fidelity satisfies

$$\max_\rho \left(F^2(\rho, \sigma) + F^2(\rho, \omega)\right) = 1 + F(\sigma, \omega).$$

The proof of this can be found in the derivation of Eq.(11) from Eq.(9) in section VI and by making use of Uhlmann's theorem.

V. OPTIMIZING OVER ALL BC PROTOCOLS

In this section, we demonstrate an upper bound on the simultaneous degrees of concealment and bindingness (hence a *lower* bound on $G^{\max}$ and $C^{\max}$) for *any* BC protocol. It should be noted that the main ideas that go into the proof of this result are present in the work of Mayers [1] and Lo and Chau [5].

Theorem 1 In any BC protocol,

$$\text{i) } G^{\max} \geq \frac{1}{2} D(\rho_0, \rho_1),$$

$$\text{ii) } C^{\max} \geq \frac{1}{2} F(\rho_0, \rho_1)^2.$$

Proof. We begin by proving (i). To analyze security against Bob, we can assume that Alice is honest. Suppose that Bob uses a strategy wherein he acts honestly throughout the commitment phase. In this case, the state of the total system at the end of this phase will be $|\psi_0\rangle$ or $|\psi_1\rangle$, depending on Alice's commitment. The reduced density operators for Bob's system will be ρ_0 or ρ_1. Now suppose that during the holding phase, Bob does the measurement which optimally discriminates between ρ_0 and ρ_1. It is a well-known result of state estimation theory [12] [13] that his information gain in this case will be

$$G = \frac{1}{2} D(\rho_0, \rho_1).$$

Bob's *maximal* information gain may be greater than this value if he also cheats during the commitment phase. For instance, it will be greater if the protocol is such that at some point during the commitment phase the reduced density operators on Bob's systems are more easily discriminated than the reduced density operators at the holding phase. However, Bob's maximal information gain cannot be less than this bound. This establishes (i).

We now prove (ii). To analyze security against Alice, we can assume that Bob is honest. Suppose that Alice uses the following strategy. During the commitment phase, she follows the honest protocol for committing a bit 0, so that, the total system is in the state $|\psi_0\rangle$ at the holding phase. Thereafter, if Alice wishes to unveil a bit 0, she acts honestly for the rest of the protocol, while if she wishes to unveil a bit 1, then she applies a unitary transformation $U^{\max}$ to the systems in her possession just prior to the unveiling phase, and thereafter acts honestly. $U^{\max}$ is chosen such that

$$\langle\psi_1| U^{\max} \otimes I |\psi_0\rangle = \max_U \langle\psi_1| U \otimes I |\psi_0\rangle. \qquad (8)$$

The probability that Alice succeeds at unveiling a bit 0 when she attempts to do so is unity, $P_{\mathrm{U}0} = 1$, since she has simply followed the honest protocol for committing a 0. The probability that Alice succeeds at unveiling a bit 1 when she attempts to do so is

$$P_{\mathrm{U}1} = Tr\left(\Pi_1 V_1 (U^{\max} \otimes I) |\psi_0\rangle \langle\psi_0| \left(U^{\max\,\dagger} \otimes I\right) V_1^\dagger\right).$$

Now since the state $|\psi_1^{\mathrm{unv}}\rangle = V_1 |\psi_1\rangle$ is an eigenstate of Π_1 with eigenvalue 1 (see Eq.(2)), one can write

$$\Pi_1 = |\psi_1^{\mathrm{unv}}\rangle \langle\psi_1^{\mathrm{unv}}| + \Gamma_1,$$

for some non-negative operator Γ_1, orthogonal to $|\psi_1^{\mathrm{unv}}\rangle \langle\psi_1^{\mathrm{unv}}|$. It follows that

$$\begin{aligned} P_{\mathrm{U}1} &\geq |\langle\psi_1^{\mathrm{unv}}| V_1 (U \otimes I) |\psi_0\rangle|^2 \\ &= |\langle\psi_1| U^{\max} \otimes I |\psi_0\rangle|^2. \end{aligned}$$

Since we are assuming that Alice is equally likely to wish to unveil a 0 as a 1, her probability of unveiling the bit of her choosing satisfies

$$\begin{aligned} P_{\mathrm{U}} &= \frac{1}{2} P_{\mathrm{U}0} + \frac{1}{2} P_{\mathrm{U}1} \\ &\geq \frac{1}{2} + \frac{1}{2} |\langle\psi_1| U^{\max} \otimes I |\psi_0\rangle|^2. \end{aligned}$$

Recalling the definition of $U^{\max}$ (Eq.(8)), and making use of Uhlmann's theorem (Eq.(7)), we conclude that Alice's control for this particular strategy satisfies

$$C \geq \frac{1}{2} F(\rho_0, \rho_1)^2.$$

Alice's maximum control may be greater than this bound, since she may be able to cheat during the commitment and unveiling phases as well, but it cannot be less. This establishes (ii). □

Corrolary 1 In any BC protocol, the optimal trade-off between $G^{\max}$ and $C^{\max}$ is a curve satisfying

$$2G^{\max} + \sqrt{2C^{\max}} \geq 1.$$

(the lower bound corresponds to curve I in Fig. 1).

Proof: This follows from Theorem 1 and Eq. (3). □

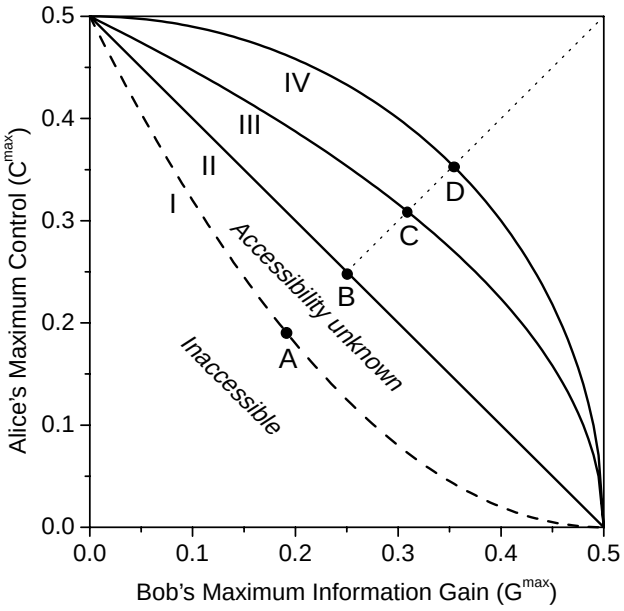


FIG. 1. Curve I is a lower bound for the trade-off relation between $C^{\max}$ and $G^{\max}$ for *any* BC protocol. The other curves are the optimal trade-off relations for Alice-supplied BC under different restrictions on ρ_0 and ρ_1: (II) no restrictions; (III) both qubit states or not both mixed states; and (IV) both pure states. A, B, C and D correspond to the points along these where the protocol is fair, i.e. $C^{\max} = G^{\max}$.

The Mayers-Lo-Chau theorem [1] [2] states that it is impossible to have a BC protocol that is both arbitrarily concealing and arbitrarliy binding, that is, one for which $G^{\max} \leq \varepsilon$ and $C^{\max} \leq \delta$ for arbitrarily small δ and ε. This clearly follows from Corollary 1. However, Corollary 1 says *more* than this, since it also sets a lower bound on the extent to which any BC protocol can be partially concealing and partially binding. Thus, in addition to being able to rule out the possibility of a BC protocol with $G^{\max}$ and $C^{\max}$ arbitrarily close to the origin in Fig. 1, one can rule out the possibility of a BC protocol anywhere below curve I of Fig. 1. The best one can hope for is a BC protocol with $2G^{\max} + \sqrt{2C^{\max}} = 1$ (curve I of Fig. 1). In particular, the best fair BC protocol one can hope for has $C^{\max} = G^{\max} = .19098$ (point A in Fig. 1).

In this paper, we do not settle the question of whether there exists a protocol for which Alice's maximal control and Bob's maximal information gain achieve the lower bounds of Theorem 1 simultaneously. Such a protocol would have to be such that Bob could not get any more information gain by cheating during the commitment phase than he can by cheating during the holding phase, and such that Alice could not get any more control by cheating during the commitment phase or the unveiling phase than she can by cheating during the holding phase. It seems to us that such a protocol is unlikely to exist.

VI. OPTIMIZING OVER ALICE-SUPPLIED BC PROTOCOLS

A. Optimal degrees of concealment and bindingness

The main results of this paper are

Theorem 2 In Alice-supplied BC protocols,

$$\text{i) } G^{\max} \geq \frac{1}{2} D\left(\rho_0, \rho_1\right),$$
$$\text{ii) } C^{\max} \geq \frac{1}{2} F\left(\rho_0, \rho_1\right).$$

Theorem 3 Purification BC protocols saturate the bounds in Theorem 2.

Proof of Theorem 2. Inequality (i) follows trivially from theorem 1, since if $G^{\max} \geq \frac{1}{2} D\left(\rho_0, \rho_1\right)$ for *all* BC protocols then clearly $G^{\max} \geq \frac{1}{2} D\left(\rho_0, \rho_1\right)$ for any Alice-supplied BC protocol.

Inequality (ii), on the other hand, is stronger than theorem 1. To prove it, we must consider Alice's most general cheating strategy. Without loss of generality, we can assume that she keeps all of her cheating actions at the quantum level. During the commitment phase, Alice can cheat by implementing a sequence of unitary operations $\{\tilde{W}_1, \ldots, \tilde{W}_n\}$ different from the honest sequence. She can cheat at the end of the holding phase by implementing a unitary transformation $U_b \otimes I$ that depends on the bit b she would like to unveil. Finally, she can cheat during the unveiling phase by implementing a sequence of unitary operations $\{\tilde{V}_{b,1}, \ldots, \tilde{V}_{b,n}\}$ that depends on the bit b she would like to unveil and that is different from the honest sequence. The maximum probability of Alice unveiling the bit of her choosing is therefore given by

$$P_{\mathrm{U}}^{\max} = \frac{1}{2} \max_{\{\tilde{W}_1, \ldots, \tilde{W}_n\}} \sum_{b \in \{0,1\}} \max_{\{\tilde{V}_{b,1}, \ldots, \tilde{V}_{b,n}\}} \max_{U_b} Tr\{\Pi_b \tilde{V}_b \left(U_b \otimes I\right) \tilde{W} \left|\psi_{\mathrm{init}}\right\rangle \left\langle\psi_{\mathrm{init}}\right| \tilde{W}^{\dagger} \left(U_b^{\dagger} \otimes I\right) \tilde{V}_b^{\dagger}\}$$

where

$$\tilde{W} \equiv W_n' \tilde{W}_n \cdots W_2' \tilde{W}_2 W_1' \tilde{W}_1, \text{ and}$$
$$\tilde{V}_b \equiv V_n' \tilde{V}_{b,n} \cdots V_2' \tilde{V}_{b,2} V_1' \tilde{V}_{b,1}.$$

$\tilde{W}$ and $\tilde{V}_b$ are the total unitary operations that Alice and Bob jointly implement given that Bob is honest and Alice cheats.

We begin by optimizing over Alice's cheating strategy during the commitment phase. It turns out that the assumption of an Alice-supplied protocol allows us to replace the maximization over $\{\tilde{W}_1, \ldots, \tilde{W}_n\}$ by a maximization over *all* unitary operations on the total system. This means that Alice has as much cheating power in an arbitrary Alice-supplied protocol as she does in a protocol where Bob does not play any role in the commitment phase. The reason is that Alice can bring about any unitary operation W by implementing the sequence of operations

$$\tilde{W}_1 = \left(W_n' \cdots W_1'\right)^{-1} W$$
$$\tilde{W}_i = I \text{ for } i \neq 1$$

This result only applies for Alice-supplied BC protocols, since Alice must initially have access to all the systems that will appear in the commitment phase in order to implement $\tilde{W}_1$. We can conclude that

$$P_{\mathrm{U}}^{\max} = \frac{1}{2} \max_{W} \sum_{b \in \{0,1\}} \max_{\{\tilde{V}_{b,1}, \ldots, \tilde{V}_{b,n}\}} \max_{U_b} Tr(\Pi_b \tilde{V}_b \left(U_b \otimes I\right) W \left|\psi_{\mathrm{init}}\right\rangle \left\langle\psi_{\mathrm{init}}\right| \times W^{\dagger} \left(U_b^{\dagger} \otimes I\right) \tilde{V}_b^{\dagger})$$

We now consider Bob's measurement. Eq.(2) implies that the honest state at the end of the unveiling phase, $|\psi_b^{\mathrm{unv}}\rangle$ must be an eigenstate of Π_b. Thus,

$$\Pi_b = \left|\psi_b^{\mathrm{unv}}\right\rangle \left\langle\psi_b^{\mathrm{unv}}\right| + \Gamma_b,$$

for some non-negative operator Γ_b. It follows that

$$P_{\rm U}^{\max} \geq \frac{1}{2} \max_{W} \sum_{b\in\{0,1\}} \max_{\{\tilde{V}_{b,1},\ldots,\tilde{V}_{b,n}\}} \max_{U_b} \left| \left\langle \psi_b^{\rm unv} | \tilde{V}_b \left(U_b \otimes I\right) W | \psi_{\rm init} \right\rangle \right|^2 .$$

Clearly the maximum over $\{\tilde{V}_{b,1},\ldots,\tilde{V}_{b,n}\}$ must be greater than or equal to the value for $\{V_{b,1},\ldots,V_{b,n}\}$, the honest sequence of operations for unveiling bit b. Thus,

$$P_{\rm U}^{\max} \geq \frac{1}{2} \max_{W} \sum_{b\in\{0,1\}} \max_{U_b} \left| \langle \psi_b^{\rm unv} | V_b \left(U_b \otimes I\right) W | \psi_{\rm init} \rangle \right|^2 .$$

Since W varies over all unitary operators, we can write $|\psi\rangle = W|\psi_{\rm init}\rangle$ and vary over all $|\psi\rangle$. Making use of the fact that $|\psi_b^{\rm unv}\rangle = V_b|\psi_b\rangle$ (Eq.(1)), we have

$$P_{\rm U}^{\max} \geq \frac{1}{2} \max_{|\psi\rangle} \sum_{b\in\{0,1\}} \max_{U_b} \left| \langle \psi_b | \left(U_b \otimes I\right) |\psi\rangle \right|^2 . \qquad (9)$$

We perform the maximization over $|\psi\rangle$ for a given U_0 and U_1. By a variational approach, it is easy to show that the optimal $|\psi\rangle$ has the form (up to an arbitrary overall phase)

$$|\psi^{\max}\rangle = \frac{\left|\tilde{\psi}_0\right\rangle + e^{-i\arg(\langle\tilde{\psi}_0|\tilde{\psi}_1\rangle)}\left|\tilde{\psi}_1\right\rangle}{\sqrt{2}\sqrt{1+\left|\left\langle\tilde{\psi}_0|\tilde{\psi}_1\right\rangle\right|}}, \qquad (10)$$

where

$$\left|\tilde{\psi}_0\right\rangle = \left(U_0 \otimes I\right)|\psi_0\rangle$$
$$\left|\tilde{\psi}_1\right\rangle = \left(U_1 \otimes I\right)|\psi_1\rangle .$$

It follows that

$$P_{\rm U}^{\max} \geq \frac{1}{2}\left(1 + \max_{U_0,U_1} \left|\langle\psi_0| U_0 U_1 \otimes I |\psi_1\rangle\right|\right). \qquad (11)$$

Inequality (ii) now follows trivially from Uhlmann's theorem and the definition of Alice's control.□

Proof of Theorem 3. Recall the definition of a purification BC protocol, defined in section III. If Alice is honest she prepares the proof-token composite in either $|\chi_0\rangle$ or $|\chi_1\rangle$ and submits the token system to Bob. In this case, the reduced density operators ρ_0 and ρ_1 that describe the token system are simply the trace over the proof system of $|\chi_0\rangle$ and $|\chi_1\rangle$, that is,

$$\rho_b = Tr_p\left(|\chi_b\rangle\langle\chi_b|\right).$$

Since Bob has no opportunity to cheat during the commitment phase, the best he can do is to try to estimate the state of the token system, that is, to discriminate ρ_0 and ρ_1. It follows from state estimation theory that his maximum information gain is $G^{\max} = \frac{1}{2}D\left(\rho_0,\rho_1\right)$ and is achieved by performing a Helstrom measurement [12] [13].

Alice can cheat in *two* ways in a purification BC protocol. She can cheat during the commitment phase by preparing the total system in a state $|\psi\rangle$ that is different from $|\chi_0\rangle$ or $|\chi_1\rangle$, and she can cheat just prior to the unveiling phase by implementing a unitary operation U_b on the proof system. The identity of U_b can of course depend on which bit b she wishes to unveil.

Recalling that $\Pi_b = |\chi_b\rangle\langle\chi_b|$, Alice's maximum probability of unveiling whatever bit she desires is

$$P_{{\rm U}b}^{\max} = \max_{|\psi\rangle} \sum_{b\in\{0,1\}} \frac{1}{2} \max_{U_b} \left|\langle\chi_b|U_b \otimes I|\psi\rangle\right|^2 .$$

Defining $\rho \equiv Tr_p\left(|\psi\rangle\langle\psi|\right)$ and making use of Uhlmann's theorem, we obtain

$$P_{{\rm U}b}^{\max} = \frac{1}{2}\max_{\rho}\left(F\left(\rho,\rho_0\right)^2 + F\left(\rho,\rho_0\right)^2\right).$$

It now follows trivially from Lemma 2 and the definition of the control that $C^{\max} = \frac{1}{2}F\left(\rho_0,\rho_1\right)$. Alice achieves this control by implementing any unitary operations U_0 and U_1 that satisfy $U_0U_1 = U^{\max}$ where $U^{\max}$ is defined in Eq.(8) and by initially preparing the state $|\psi^{\max}\rangle$ of Eq.(10) with $|\psi_b\rangle = |\chi_b\rangle$. □

B. Optimal trade-off relations

Given theorem 3, it is straightforward to determine the optimal trade-off relations between $G^{\max}$ and $C^{\max}$ for various restrictions on the states of Bob's system at the holding phase.

Corrolary 2 In Alice-supplied BC protocols where ρ_0 and ρ_1 are arbitrary, the optimal trade-off is

$$C^{\max} + G^{\max} = \frac{1}{2}$$

(This corresponds to curve II in Fig. 1).

Proof. This follows from theorem 3 and Eq.(3). □

Corrolary 3 In Alice-supplied BC protocols where ρ_0 and ρ_1 either (1) have supports that lie in a single 2 dimensional Hilbert space, or (2) are not both mixed, the optimal trade-off is

$$2(C^{\max})^2 + G^{\max} = \frac{1}{2}.$$

(This corresponds to curve III in Fig. 1).

Proof. This follows from theorem 3, Eq.(6) and Lemma 1. □

Corrolary 4 In Alice-supplied BC protocols where ρ_0 and ρ_1 are both pure states, the optimal trade-off is

$$(C^{\max})^2 + (G^{\max})^2 = \frac{1}{4}.$$

(This corresponds to curve IV in Fig. 1).

Proof. This follows from theorem 3 and Eq.(5). □

We now provide simple examples of protocols that achieve the optimal trade-offs of Corollaries 2-4.

To achieve the optimal trade-off of Corollary 2, it suffices to consider a purification BC protocol where ρ_0 and ρ_1 saturate the inequality of Eq.(3). The simplest example makes use of commuting density operators in a 3 dimensional Hilbert space. Specifically,

$$\rho_0 = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } \rho_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}.$$

It is straightforward to show that $D(\rho_0, \rho_1) = \lambda$ and $F(\rho_0, \rho_1) = 1 - \lambda$, which implies that $D(\rho_0, \rho_1) + F(\rho_0, \rho_1) = 1$. It follows that this example provides a family of protocols that achieve the optimal trade-off for Alice-supplied BC protocols where ρ_0 and ρ_1 are arbitrary.

We now provide a specific example of a family of protocols that achieve the optimal trade-off of Corollary 3. We consider purification BC protocols wherein

$$\rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } \rho_1 = \begin{pmatrix} \lambda & 0 \\ 0 & 1-\lambda \end{pmatrix}.$$

Note that this example qualifies both as an example where ρ_0 and ρ_1 have supports that lie in the same 2 dimensional Hilbert space, and as an example where one of ρ_0 and ρ_1 is pure. It is easy to see that $D(\rho_0, \rho_1) = 1 - \lambda$ and $F(\rho_0, \rho_1) = \sqrt{\lambda}$. Thus, we have saturated the lower bound in Eq.(6) and lemma 1, and consequently, this family of protocols is optimal for the specified restrictions of ρ_0 and ρ_1.

It is trivial to find BC protocols that achieve the optimal trade-off of Corollary 4. Any purification BC protocol where ρ_0 and ρ_1 are pure states will do. Specifically, if

$$\rho_0 = |0\rangle\langle 0| \text{ and } \rho_1 = |\phi\rangle\langle\phi|,$$

where $|\phi\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle$, then one achieves every point on the curve $(C^{\max})^2 + (G^{\max})^2 = \frac{1}{4}$ by varying over all ϕ in the range 0 to $\pi/2$.

If we define a 'fair' BC protocol to be one where $C^{\max} = G^{\max}$, then by substituting this identity into the trade-off relations presented above, we obtain the following results. The best fair BC protocol from among the class of Alice-supplied BC protocols has $C^{\max} = G^{\max} = 0.25$ (point A on Fig. 1). The best fair BC protocol from among the class of Alice-supplied BC protocols where ρ_0 and ρ_1 are both qubit states or at least one of ρ_0 and ρ_1 is pure has $C^{\max} = G^{\max} = \frac{\sqrt{5}-1}{4} \simeq .30902$ (point B on Fig. 1). Finally, the best fair BC protocol from among the class of Alice-supplied BC protocols where ρ_0 and ρ_1 are both pure states has $C^{\max} = G^{\max} = \frac{1}{2\sqrt{2}} \simeq .35355$ (point C on Fig. 1).

VII. SIGNIFICANCE FOR COIN TOSSING

We briefly discuss the relevance of these results to coin tossing [5] [6] [14]. Coin tossing(CT) is a cryptographic task wherein at the end of the protocol both parties perform a measurement that has three outcomes corresponding to Alice winning, Bob winning, and the other party being caught cheating. If neither party is caught cheating, then the two measurements must agree on who won the coin toss. We can define a party's bias in a coin tossing protocol as the difference between their probability of winning and 1/2. A CT protocol with maximum bias α for Alice and maximum bias β for Bob is one where if Bob is honest, the maximum Alice can make her probability of winning is $\frac{1}{2} + \alpha$, and if Alice is honest, the maximum Bob can make his probability of winning is $\frac{1}{2} + \beta$. Coin tossing can be built upon BC as follows. After the commitment phase, Bob sends Alice a bit which represents his guess of her commitment. If his guess corresponds to the bit Alice unveils, he wins the coin toss; if not, Alice wins. Our results show that it is possible to build a secure CT protocol for any pair of biases satisfying $\alpha + \beta \geq 1/2$, and that this inequality can be saturated. In particular, a fair CT protocol with bias of 1/4 can be built up in this way.

Since CT is a weaker primitive than BC [14], the impossibility of a BC protocol that is arbitrarily concealing and binding does *not* imply the impossibility of a CT protocol with arbitrarily small biases for both parties [15]. Whether such a protocol is possible remains an open question in quantum cryptography.

It should be noted that even if such a CT protocol does not exist, the fact that there exist CT protocols with bounded biases for both parties is still potentially very useful. For instance, these can provide protocols for gambling [16] wherein both parties (the casino and the gambler) can be assured that their probability of winning is greater than some bound, regardless of the actions of the other party.

VIII. CONCLUSION

We have studied the extent to which BC protocols can be made simultaneously both partially concealing and partially binding. The degrees of concealment and bindingness were quantified by Bob's maximum information

gain about the bit committed and Alice's maximum control over the bit she unveils. A lower bound on Alice's maximal control and Bob's maximum information gain for *any* BC protocol has been derived, although it is not known whether or not this bound can be saturated. A stronger lower bound was obtained for a restricted class of BC, called 'Alice-supplied' protocols, wherein Alice provides Bob with all of the systems that he makes use of during the commitment phase. Moreover, this lower bound has been shown to be saturated by what we have called a 'purification' BC protocol, wherein an honest Alice must prove her commitment to Bob by providing him with a purification of the state she submitted to him during the commitment phase.

Finally, we have considered the trade-off between concealment and bindingness for Alice-supplied BC protocols given different constraints on ρ_0 and ρ_1 (these are the states of the systems in Bob's possession during the holding phase given commitments of 0 and 1 respectively). Such constraints might arise from practical restrictions on the physical implementation of a BC protocol. We have shown that for BC protocols where ρ_0 and ρ_1 have supports in a single 2D Hilbert space, or wherein ρ_0 and ρ_1 are not both mixed, one cannot achieve the optimal trade-off relation (that is, the optimal degree of bindingness for every degree of concealment). Using protocols wherein ρ_0 and ρ_1 are both pure, one does even worse. The optimal trade-off for Alice-supplied BC protocols is $C^{\max}+G^{\max} = \frac{1}{2}$ and can be achieved using a purification BC protocol wherein ρ_0 and ρ_1 are mixed but commuting states of a 3-dimensional Hilbert space.

The following question concerning the degrees of concealment and bindingness in BC protocols remains unanswered: do there exist any BC protocols with a trade-off relation that is better than the linear trade-off relation $C^{\max} + G^{\max} = \frac{1}{2}$? In order to settle this question, the scope of our analysis must be extended beyond Alice-supplied protocols. We conjecture that the linear trade-off is in fact the optimal trade-off from among *all* BC protocols.

Note added. After the completion of this research the authors were informed [17] of related results obtained by A. Ambainis on fair coin tossing protocols with bounded biases.

IX. ACKNOWLEDGMENTS

This work was supported by the National Science and Engineering Research Council of Canada, the Austrian Science Foundation FWF, and the TMR programs of the European Union Project No. ERBFMRXCT960087.

[1] D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997).

[2] H.-K. Lo and H. F. Chau, *Phys. Rev. Lett.* **78**, 3410 (1997).

[3] In this paper, we consider only BC protocols that can be implemented between parties who both have only a single laboratory that is localized in space. Kent has shown [4] that unconditionally secure BC *can* be achieved if one relaxes this constraint, for instance, if both parties have a pair of laboratories separated by a distance L (so that there are four laboratories in all), each of which can be verified to be a distance d to one of the other party's laboratories, with $d \ll L$. The security stems from the constraint imposed by special relativity on the speed of communications between a party's two laboratories. Unfortunately, the protocol requires a channel capacity that increases exponentially with the duration of the holding phase.

[4] A. Kent, *Phys. Rev. Lett.* **83**, 1447 (1999).

[5] H.-K. Lo and H. F. Chau, *Physica D*, **120,** 177 (1998).

[6] D. Aharonov *et al.*, quant-ph/0004017.

[7] The degree of concealment quantifies the extent to which the protocol prevents Bob from gaining information about Alice's commitment. This is the standard notion of security against Bob in BC. Nonetheless, there are cryptographic tasks(such as coin tossing) wherein it is useful to consider a *different* type of security against Bob, namely, *cheat detection.* A protocol with this type of security ensures that if Bob gains any information about Alice's commitment then Alice has some finite probability of detecting that he has done so. We shall not consider this type of security here, however, see L. Hardy and A. Kent, quant-ph/9911043.

[8] R. W. Spekkens and T. Rudolph, 'Optimization of coherent attacks in generalized BB84 bit commitment protocols', in preparation.

[9] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[11] R. Josza, *J. Mod. Opt.* **41**, 2315 (1994).

[12] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[13] C. A. Fuchs, *Distinguishability and Accessible Information in Quantum Theory,* Ph.D. thesis, University of New Mexico, Albuquerque, NM, 1996.

[14] A. Kent, *Phys. Rev. Lett.* **83**, 5382 (1999).

[15] Again, we are only considering protocols that can be implemented between localized parties, as discussed in Ref. [3]. It has been shown by Kent [14] that if one relaxes this constraint, unconditionally secure coin tossing with arbitrarily small biases can be achieved.

[16] L. Goldenberg, L. Vaidman and S. Wiesner, *Phys. Rev. Lett.* **82,** 3356 (1999).

[17] G. Brassard, private communication at the Summer School in Quantum Information Processing, The Fields Institute, Toronto, May 14-18, 2001.

X. APPENDIX

Proof of Lemma 1. The density operators for qubits can be represented by vectors on the Bloch sphere. If ρ and σ are represented by vectors $\vec{r}$ and $\vec{s}$, then in terms of these, the trace distance and fidelity squared can be written as [10] [11]

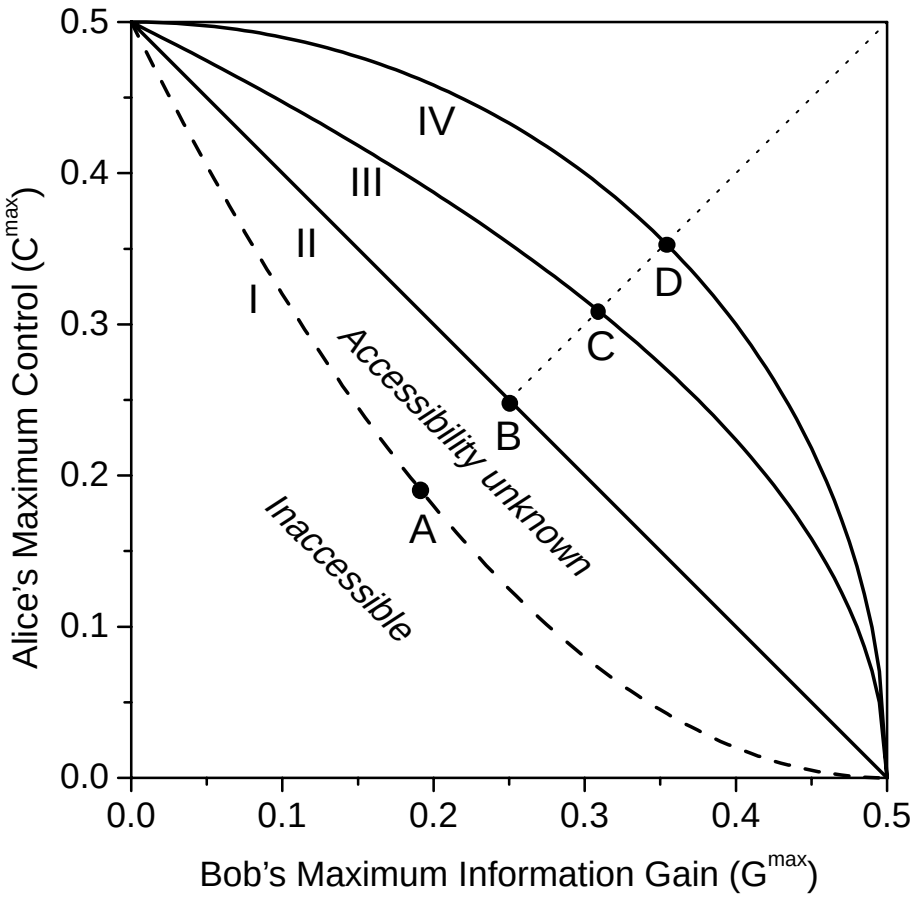
$$D(\rho,\sigma) = \frac{1}{2}\left|\vec{r}-\vec{s}\right|,$$
$$F^2(\rho,\sigma) = \frac{1}{2}\left(1+\vec{r}\cdot\vec{s}+\sqrt{\left(1-\left|\vec{r}\right|^2\right)\left(1-\left|\vec{s}\right|^2\right)}\right).$$

2

Defining $r = \left|\vec{r}\right|, s = \left|\vec{s}\right|$ and $\cos\phi = \vec{r}\cdot\vec{s}/rs$, we have

$$D+F^2 = \frac{1}{2}\sqrt{r^2+s^2-2rs\cos\phi} + \frac{1}{2}\left(1+rs\cos\phi+\sqrt{\left(1-r^2\right)\left(1-s^2\right)}\right).$$

This is minimized for $\phi = 0$. Moreover, assuming (arbitrarily) that $r \geq s$, we have $\sqrt{r^2+s^2-2rs} = r-s$ and $\sqrt{\left(1-r^2\right)\left(1-s^2\right)} \geq (1-r)(1+s)$. Together, these facts imply $D(\rho,\sigma)+F(\rho,\sigma)^2 \geq 1$. □


0.5
0.4
0.3
0.2
0.1
0.0
0.0
0.1
0.2
0.3
0.4
0.5
Alice's Maximum Control (C^{max})
Bob's Maximum Information Gain (G^{max})
IV
III
II
I
D
C
B
A
Accessibility unknown
Inaccessible